# Diskreter Logarithmus

Josef Schmeißer und Fabian Grotz

25.05.2016

Sei $(\mathbb{G}, \cdot)$ eine Gruppe, wir definieren:

## Definition

- $e$ bezeichnet das neutrale Element
- $ord(\mathbb{G}) := |\mathbb{G}|$
- Für $\alpha \in \mathbb{G}$ ist $ord(\alpha) = n$ mit $\alpha^n = e$

## Definition

Sei $n \in \mathbb{N}$ und $\alpha^n = 1$ sowie $\alpha^{n/p} \neq 1$ für alle Primteiler $p$ von $n$. Dann hat $\alpha$ die Ordnung $n$.

## Definition

Eine Gruppe $\mathbb{G}$ heißt zyklisch, wenn ein $g \in \mathbb{G}$ existiert, so dass:

$$\forall \alpha \in \mathbb{G} : \exists i \in \mathbb{N} : g^i = \alpha$$

Wir nennen $g$ einen Generator der zyklischen Gruppe.

- Sei $(\mathbb{G}, \cdot)$ eine Gruppe und $\alpha \in \mathbb{G}$.
- $\alpha$ sei von endlicher Ordnung.

**Definition**

$\langle \alpha \rangle$ bezeichnet die von $\alpha$ erzeugte Untergruppe.

Die Euler'sche $\varphi(n)$-Funktion ist wie folgt definiert:

**Definition**

Sie gibt für eine natürliche Zahl $n$ an, wie viele zu $n$ teilerfremde natürliche Zahlen existieren, welche nicht größer als $n$ sind:

$$\varphi(n) := \left|\{a \in \mathbb{N} \,|\, 1 \leq a \leq n \wedge ggT(a,n) = 1\}\right|$$

Sei $\mathbb{G}$ die prime Restklassengruppe $(\mathbb{Z}/p\mathbb{Z})^{\times}$ mit der Multiplikation als vorherrschende Operation (gekennzeichnet durch $\times$).

**Definition**

Ein Element $\alpha \in \mathbb{G}$ ist eine Primitivwurzel modulo $p$, wenn gilt:

$$ord(\alpha) = \varphi(p)$$